Short Public Report

Application No.: 20130802 Valid-ZLC®

1. Name and version of the IT product:*

Name of Product	:	Valid-ZLC® (ValidSoft's "Zero Latency Correlation" product to assist banks in their „[bank] card-present" anti-fraud measures)
Product Description	:	The product, Valid-ZLC®, is a tool that allows the user of the product, a bank or payment processor, to check if a bank card that is being presented for a payment, is in the same country as the bank card holder's mobile phone. This greatly enhances the efficacy of the user's anti-fraud measures. *This is the sole purpose of the Valid-ZLC® product.*
Version	:	Version 2, August 2013

*Notes:

1) The product is essentially software, but is operated and managed by ValidSoft as "Software as a Service".

2) This product is not currently offered under any other names, but this may be done in future.

2. Manufacturer of the IT product:

Company Name:

ValidSoft UK Ltd.

Company Address:

ValidSoft (UK) Ltd
9 Devonshire Square
London EC2M 4YF
United Kingdom

Contact Persons and Contact Details:

Mr. Pat Carroll, CEO, Validsoft UK Ltd
Alexander Korff, Esq., Legal Counsel for ValidSoft UK Ltd
Address as above.
E: Pat.Carroll@validsoft.com, alexander.korff@elephanttalk.com

3. Time frame of evaluation:

June 2013 – July 2014

4. EuroPriSe Experts who evaluated the IT product:

Name of the Legal Expert:

Prof. Douwe Korff

Address of the Legal Expert:

Wool Street House, Gog Magog Hills, Babraham, Cambridge CB22 3AE, UK

Name of the Technical Expert:

Javier Garcia-Romanillos Henriquez de Luna

Address of the Technical Expert:

Ernst & Young (Spain)
Plaza Pablo Ruiz Picasso 1, Torre Picasso, 28020, Madrid, Spain

5. Certification Authority:

Name:

EuroPriSe GmbH

Address:

Joseph-Schumpeter-Allee 25
D-53227 Bonn
Germany

6. Specification of Target of Evaluation (ToE):

As described at 7, below, Valid-ZLC® checks, at the request of banks that have issued credit- or debitcards to certain customers, and who have enrolled those customers (card holders) in a relevant anti-fraud scheme, when a card of such an enrolled customer is presented for payment in a country, whether the mobile phone of that customer is also in that country (or not), by correlating the country information received from the phone* against the information on the country where the relevant payment is being made, received from the bank. (See also the Chart at 12, below).

*Note: Although the bit of software that must be installed on the mobile phone to instruct it to send the country information to the main Valid-ZLC® system operated by ValidSoft in certain instances can be installed on the phone as a standalone instruction, in practice banks will usually already have provided to the relevant customers a special "mobile banking application" (Mobile Banking App) for installation on the customers' mobile phones. In such a typical case, the small bit of software to be installed at the phone for the ZLC product (the "ZLC snippet") would be installed as an optional add-on or update to that mobile banking App.

The evaluation covered the following:

- the specifications for the bit of software (the "ZLC snippet") that banks should use to instruct the App that is installed on their enrolled customers' mobile phones to send country information to the ZLC "box" operated by ValidSoft in certain

specified instances. Since the product is not yet in any actual deployment, the experts could not evaluate any actual App. However, they did evaluate a test version of the App.;

- the parameters (security/encryption specifications) specified by ValidSoft for the data flows to and from the ZLC "box" (i.e., for the sending of the mobile phone country information from the App to the "box"; the sending of the card country information from the bank to the "box"; and the returning of a "result" from the "box" to the bank); and
- all the processing within the ZLC "box", i.e., the receiving of the above-mentioned country information from, respectively, the App and the bank; the correlation of those data within the "box", leading to the creation of "results" (in the format "Yes" [mobile phone is in the same country as the card], "No" [mobile phone is not in the same country as the card], or "Fail" [when for some reason the check could not be performed], with a "confidence score").

The above scope of the evaluation, and its limitations, are indicated by red dotted lines in the Chart in section 12, below (see the Legenda under the chart).

7. General description of the IT product:

Background

Plastic Card fraud has reached unprecedented levels around the world. Card fraud on EU issued cards alone is running at around €1.5 billion Euros per year, of which €600 million Euros is attributed to card-present fraud.

Current detection and prevention technology is based on risk engines operated by the banks that typically analyse transactions based on historical spending patterns/activity. This approach results in high false positives: when transactions are declined as probably fraudlent when in fact they are genuine. As a consequence the bank is forced to limit the amount of transactions it can check for fraud in order to balance the cost of resolution vs actual fraud. This approach means that thousands of fraud transactions slip through the net.

The product

Like the other ValidSoft products that had already previously been awarded the *EuroPriSe* seal, Valid-ZLC® is a tool to assist banks in identifying suspicious (i.e., possibly fraudulent) credit- and debitcard "card-present" transactions at Automated Telling Machines (ATMs or "cashpoints") and at Point of Sale (POS) terminals, as used in supermarkets, retailers, restaurants, etc., etc..

ZLC in Valid-ZLC® stands for "**Zero Latency Correlation**". This refers to the fact that this ValidSoft product correlates data about the country where a data subject's mobile phone is, with data on where that same data subject's bank card is, without any delay (latency) caused by mobile networks, such as occurs in correlation checks using GPS location or in products which rely on real-time mobile network interrogation.

Basically, Valid-ZLC® verifies, with the help of data previously obtained from the data subject's mobile phone, whether the card that is being presented is, or is not, in the same country as the mobile phone that the card owner has registered with the bank. Those data are sent to Valid-ZLC® as a result of the inclusion of certain ZLC code snippets into the software code operating a client's device such, typically, the relevant bank's mobile banking application ("App")

As illustrated in the Chart at 12, below, Valid-ZLC® is essentially a software program installed on a dedicated carrier or server installed at and operated by ValidSoft in the UK. The software is in effect a proprietary database, a virtual "box" developed by ValidSoft, to and from which data are sent and managed. Specifically, this "box", on the one hand receives data from mobile phones enlisted to the service by the bank/user of Valid-ZLC®, and on the other hand is linked to the client's own computers. This software is provided by ValidSoft as "Software-as-a-Service (or SaaS).

Valid-ZLC® significantly enhances the trust that banks and payment processors can have in their "risk engines", by helping them eliminate a large proportion of "false positives", in which the risk engine wrongly identifies a transaction as probably fraudulent when in fact it is genuine.

8. Transnational issues:

Transborder data flows

The user of the TOE (i.e., the bank or payment processor in question) can be established anywhere, either within or outside the EU/EEA. The ZLC "box" will always be hosted by ValidSoft, in the UK.

If the user is also in the EU/EEA, there are no data flows that are subject to the restrictions and exceptions stipulated in Articles 25 and 26 of the Data Protection Directive.

If the user is based outside the EU/EEA, the data flow in which the "box" send the "results" of the correlation to the client is a transborder data flow that is subject to those articles. However, the experts felt that they did not need to examine this scenario in detail, because whatever the scenario, the transborder data flow that is subject to those articles, is always allowed on the basis of the free and informed consent of the data subjects (Article 26(1)). However, they noted that in this scenario, the only data that are sent to the client/user outside the EU/EEA are the "result" data, i.e., whether the bank card that is being used is in the same country as the mobile phone in question (with a transaction number and a probability score).

Applicable law

The main Directive stipulates in Article 4 what is to be the "applicable law" in respect of any personal data processing operation. If the processing takes place "in the context of the activities of" an establishment of a controller, and that establishment is in the EU/EEA, then the law of the country where that establishment is, will be the "applicable law" (Article 4(1)(a) of the Directive). If there is no EU/EEA establishment, the controller must comply with the law of any EU/EEA State where he uses "means" to carry out the processing, unless this only involves transit of the data through the EU/EEA.

Unfortunately, the implications of the approach of the Article 29 Working Party to the question of "joint controllers" for the issue of "applicable law" has not yet been clarified.

The experts felt that with regard to software offered as a service (SaaS), and more specifically with regard to the Valid-ZLC® product, the most appropriate approach is to hold that the law of the country of establishment of a provider of an SaaS in the EU/EEA is the "applicable law" with regard to the processing of personal data for which that provider is the main controller, while the law of the country of establishment

of any user of the SaaS who is established in the EU/EEA is the "applicable law" for the processing for which the user of the SaaS is the main controller; and the law of the country of establishment of the provider of the SaaS is the "applicable law" for any processing by any user of the SaaS who is based outside the EU/EEA.

In the case of the Valid-ZLC® product, ValidSoft has the main responsibility for the processing of the data within the ZLC "box" and in relation to the receiving and sending of data that are under its control, while the client/user of the product (the bank) has the main responsibility for the processing by means of the App, and the sending and receiving of data to and from the ZLC "box" that are under its (the bank's) control.

This means that if the client/user of the product is established outside the EU/EEA, UK data protection law (the UK Data Protection Act) applies both to all the processing of personal data for which the client/user is mainly responsible, and to all the processing of personal data for which ValidSoft, as the SaaS provider, is mainly responsible; but that if the client/user of the product is established within the EU/EEA, the law of the country of establishment of the client/user applies to the processing of personal data for which the client/user is mainly responsible, while the UK DPA applies to the processing of personal data for which ValidSoft, as the SaaS provider, is mainly responsible – except that, insofar as ValidSoft must also be regarded as a processor, ValidSoft must in the latter case meet the data security standards of both the UK and of the country of establishment of the client/user of the product (Article 17(3)(2) of Directive 95/46/EC).

The Conditions of Use stipulate the above for these two scenarios, and the experts concluded that compliance with those conditions ensures compliance with the relevant requirements in both scenarios.

9. Tools used by the manufacturer of the IT product:

The product is provided as Software-as-a-Service (SaaS) by the developer, ValidSoft. It essentially consists of a relatively simple software programme installed on a dedicated carrier or "box", hosted by ValidSoft (in the UK). The ZLC "box", hosted by ValidSoft, receives information from, on the one hand, the "risk engine" of the client (bank) on whose behalf the checks carried out by the product are made, and on the other hand, from an App installed on the data subjects' mobile phones (with their full, free and informed consent). See the illustration in section 12, below.

The main system – the software that comprises the "box" – is written in Java.

Note: When we refer to the product as a "box", this is only for ease of reference and to enable the reader to envisage the processing: the product as such really only consists of software; the "box" referred to is thus a purely virtual "box". For that reason, the word is always placed in quotation marks.

ValidSoft is in charge of backups and restoration of data/databases as required. ValidSoft is also responsible for all technical and organisational measures relating to the processing within the ZLC "box", the receiving and sending of data by and from the "box", and the physical environment around the "box", but the constraints are to be defined by the client. The software also facilitates relevant user access management by ValidSoft. The software also facilitates encryption of the internal databases.

10. Edition of EuroPriSe Criteria used for the evaluation:

EuroPriSe Commentary, version May 2014.

11. Evaluation results:

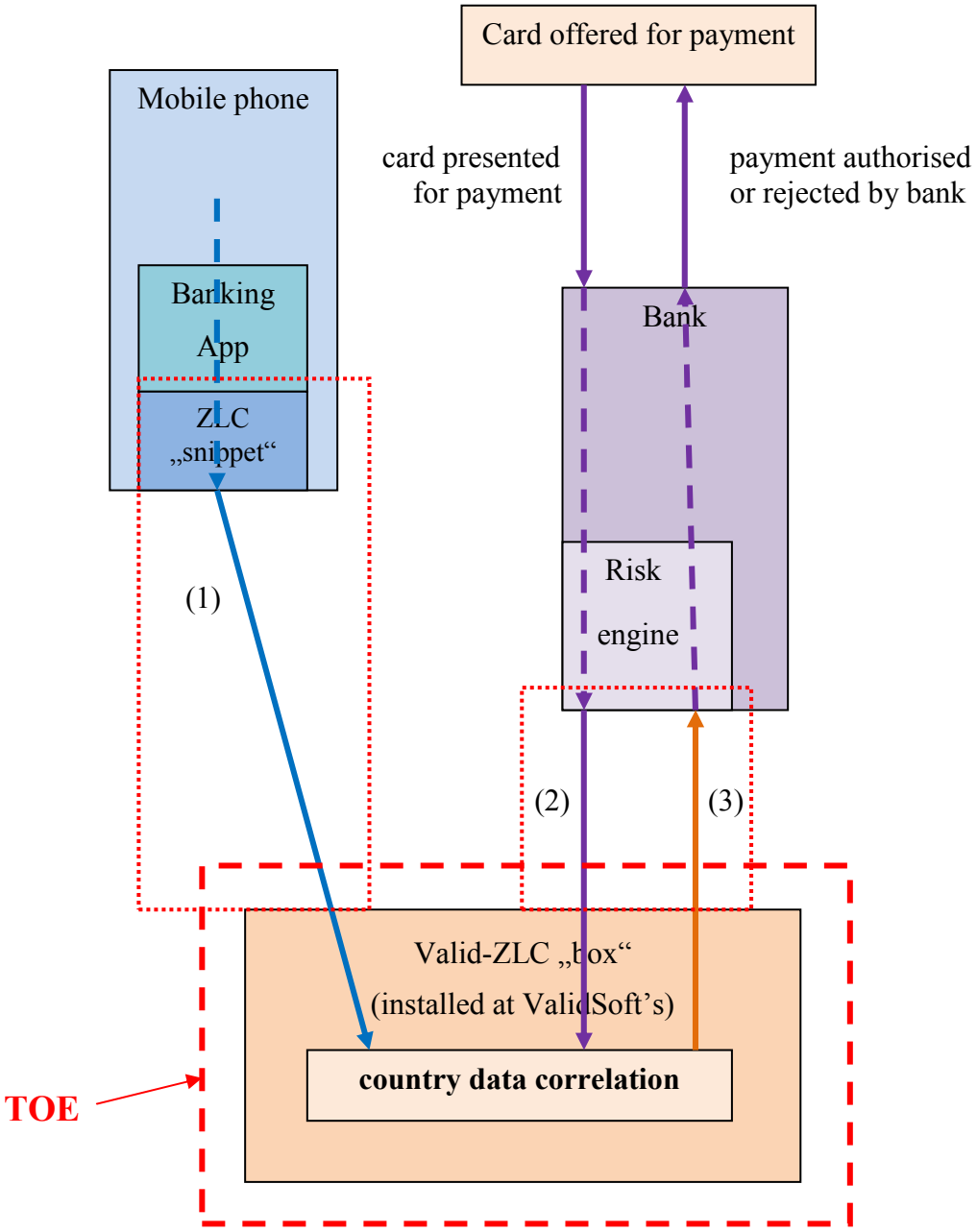
The experts concluded that the product should be rated "excellent" or "fully permitted" on the following issues in particular:

- **Data avoidance and -minimisation, pseudonymisation and anonymisation, internal data disclosures, and proportionality:** The product uses extremely limited personal data. The ZLC „snippet" only passes on to the ZLC „box" the country code of the country where a mobile phone is, and even that only if this information changes (or has not changed for some 12 hours). Moreover, the data that are made accessible to the end-user of the product are restricted to no more than a simple "result": "Confirm" (the mobile phone is in the same country as the country in which the bank card is being presented) or "Refute" (the phone is not in the same country), with a Probability Score (or a „Fail" in case the check was unsuccesful). This is moreover done without any delay ("latency"). These data minimisation measures constitute a strongly privacy-enhancing feature that ensures that the product can really only be used for the very specific, limited and manifestly legitimate purpose of fraud detection and –prevention, and cannot be used to create a longitudinal profile of a person's movements (even across borders).
- **Transparency and description of the SaaS:** This is ensured through detailed product documentation, in particular in the form of the Core Model Product Guide.
- **Legal basis:** All the processing is fully permitted on the basis of the free and specific, informed consent of the data subjects; this is strongly reinforced by the strong provisions on the informing of the data subjects and the obtaining of their consent in the Conditions of Use for the product.
- **Purpose-specification and –limitation:** The very limited, but important, purpose of the product is well-defined: to check if the mobile phone of the data subject is in the same country as the country where that same data subject's bank card is being presented to make a payment or to withdraw cash; and the arrangements ensure that the very limited data that are generated can only be used for this clear, specific purpose.
- **Quality of data:** The "results" generated by the product are highly reliable, as long as the data subject does not switch his or her App off.
- **Transfers to third countries:** All the transborder data transfers that need to be assessed under Article 25 and 26 of the Data Protection Directive are fully covered by the informed consent of the data subjects.
- **Legal arrangements:** As far as this can be done by means of legal stipulations, the Conditions of Use ensure full compliance with all relevant data protection requirements on the part of the user of the product, including the requirements on the informing of data subjects and the obtaining of their consent. The template contract between the developer of the product, ValidSoft, and the user of the product (the bank) also fully meets the relevant European data protection rules, in particular on controller – processor contracts.

The Experts therefore concluded that overall, Valid-ZLC® both improves the efficacy of anti-fraud measures by banks and ensures protection of individual privacy and data protection, in a way that fully meets European data protection standards.

12. Data flows:

The chart below outlines the main data flows relating to the use of the Valid-ZLC® product:



Legenda:

(1) Country information sent from the App to the ZLC “box”“
(2) Country information sent from the bank to the ZLC “box”“
(3) „Result“ returned to the bank from the ZLX “box”“ (Y/N/F + score)
– – – Main scope of evaluation (processing within the ZLC “box”“)
..... Issues evaluated in terms of parameters/specifications only (ZLC “snippet”; security/ encryption parameters for data flows from App and from bank to the ZLC “box”)

13. Privacy-enhancing functionalities:

As already mentioned at 11, above, the EuroPriSe experts concluded that the product should be rated "excellent" or "fully permitted" on the following issues in particular:

- Data avoidance and -minimisation, pseudonymisation and anonymisation, internal data disclosures, and proportionality;
- Transparency and description of the SaaS;
- Legal basis;
- Purpose-specification and –limitation;
- Quality of data;
- Transfers to third countries; and
- Legal arrangements.

The experts therefore concluded that overall, Valid-ZLC® both improves the efficacy of anti-fraud measures by banks and ensures protection of individual privacy and data protection, in a way that fully meets European data protection standards.

14. Issues demanding special user attention:

The experts have identified no issues demanding special user attention.

15. Compensation of weaknesses:

The experts have identified no weaknesses in the product that demand compensatory action.

16. Decision table on relevant requirements:

EuroPriSe Requirement	*Decision*	*Remarks*
Data Avoidance and Minimisation	excellent	The App only sends a country code to the ZLC "box", and only at relevant specified instances. This happens when the phone is switched on or when, after the provision of location data by means of the App has been disabled, this is re-enabled, or when the phone connects to a mobile network in another country than its country of registration, or when none of these has happened for 12 hours. When this happens, the previous information is deleted, i.e., there is no chronological record of the data subjects' movements over time, even between countries: all that is recorded at any time is the country in which the enrolled phone (the registered device) is at that time. Moreover, the bank only receives a "Confirm" or "Refute" (or "Fail") message, that is only useful for the specific purpose of fraud prevention

16. Decision table on relevant requirements (continued):

Transparency	excellent	The product/SaaS is very well described in the Core Model Product Guide. Transparency *vis-à-vis* the data subjects is as well ensured as can be done, by means of the Conditions of Use which are strict in this regard, and through eccellent template information notices provided in the CMPG.
Technical-Organisational Measures	adequate	Although the arrangements on paper (Conditions of Use and warranties) for these measures were very good, the product was only given the rating of "adequate" because the quality of the actual measures cannot be assessed until the product (the SaaS) is in actual deployment.
Data Subjects' Rights	adequate	Again, although the arrangements on paper (Conditions of Use and warranties) in this respect were very good, the product was only given the rating of "adequate" because the quality of the actual measures cannot be assessed until the product (the SaaS) is in actual deployment.

Experts' Statement

We affirm that the above-named IT product has been evaluated according to the EuroPriSe Criteria, Rules and Principles and that the findings as described above are the result of this evaluation.

[signature sent by post]

Prof. Douwe Korff (legal Expert)

Cambridge, UK, 5 August 2014

[signature sent by post]

Javier Garcia-Romanillos Henriquez de Luna (Technical Expert)

Madrid, Spain, 5 August 2014

Certification Result

The above-named IT product passed the EuroPriSe evaluation.

It is certified that the above-named IT product facilitates the use of that product in a way compliant with European regulations on privacy and data protection.

Place, Date	Name of Certification Authority	Signature